REMARKS

The applicant has amended claim 1 to specifically recite that the boot method of claim 1 either polls the serial port for activity or jumps to flash memory for execution of boot instructions stored in the flash memory. The preamble of claim 1 also now recites that the flash memory stores both boot instructions and a key value stored in a security location, and that the internal, read-only memory stores boot program code and a predetermined security value, and that it is the boot program code stored in the read-only memory that performs the boot method steps. Amendments to original method claims 3, 6, 7, and 8 are consequential to these amendments. Claim 1 currently provides:

> 1. A boot method for use in a mobile device having FLASH memory storing boot instructions and a key value stored in a security location, having an internal read-only memory storing boot program code and a predetermined security value, and having a serial port, the boot program code stored in the read-only memory performing the steps of:
>
> reading a key value from a security location in the FLASH memory;
>
> comparing the key value to a predetermined security value stored in the internal read-only memory; and
>
> depending on the result of the comparison of the key value to the predetermined security value, either polling the serial port for activity or jumping to the FLASH memory for execution of boot instructions stored therein.

Claim 8 has been amended to recite a processor for use in a mobile device which operates in a manner consistent with claim 1:

> 8. A processor configured to communicate with internal read-only and FLASH memories of an apparatus for use in a mobile device having a serial port, the processor being configured to execute boot program code stored in a read-only memory for reading a key value from a security location in a FLASH memory, and for comparing said key value to a predetermined security value stored in the internal read-only memory, and, depending on the result of the comparison of the key value to the predetermined security value, either polling the serial port for activity or jumping to the FLASH memory for execution of boot instructions stored therein.

Currently amended claim 9 recites an apparatus for use in a mobile device, comprising the processor of claim 8. Other amendments to the apparatus claims 10, 11, 14, and 17 are consequential to the amendments to claims 8 and 9.

Support for the currently amended claims may be found at paragraphs 7-9, 23 and 35 of the specification as originally filed.

The Examiner rejected the claims as filed on the basis of US 6,138,236 (Mirov et al) in view of US 5,805,882 (Cooper et al). The applicant notes that both references were cited in the IDS previously filed by the applicant in this application, although the Mirov reference was cited as the corresponding EP document. The applicant respectfully traverses the Examiner's rejection, and submits that claims 1 through 20 are patentable over the cited art for the following reasons:

Mirov does not teach comparing a key value to a predetermined security value stored in internal memory

The Examiner stated that Mirov taught "comparing the key value to a predetermined security value stored in the internal memory", because Mirov taught "comparing verification hash with data hash, col. 4, lines 18-26 and col. 5, lines 6-15" (Detailed Action dated September 27, 2006, page 2). The applicant disagrees. Mirov does not teach "comparing" a value with another predetermined value "stored" in the internal memory; moreover, Mirov does not teach that a comparison is carried out with a "predetermined security value", as recited in claim 1.

In claim 1, the predetermined security value is stored in the internal read-only memory that also stores boot program code. (While claim 1 as originally filed recited "internal memory", it would be understood by a person skilled in the art that said memory was read-only; in a preferred embodiment, the memory is an internal BootROM, as described in paragraph 25 of the present application. The currently amended claims emphasize the read-only nature of the internal memory.) But Mirov does not teach that the read-only memory (which is the "authentication section" 45 in Figure 2, described as ROM in col. 3, lines 59-60) stores any predetermined value that is compared to any other value. Rather, Mirov teaches that:

> During initialization of the computer system 10, the secure micro-code 51 of the authentication section 45 executes and directs the hash generator 53 to generate a data hash of the unsecured micro-code 58 programmed in the programmable section 55 of the flash PROM 18. The secure micro-code 51 also directs the decryptor 54 to calculate a verification hash. The decryptor applies the public key 56 of the authentication section 45 and the digital signature 57 of the programmable section 55 and calculates the verification hash.
>
> Once the verification hash and the data hash are generated, the micro-code 51 directs the comparator 52 to compare the verification hash with the data hash. (col. 4, lines 8-20)

There is thus no predetermined value in the read-only memory. There is a decryptor that calculates a verification hash, and a hash generator that generates a hash of the unsecured code in the flash PROM; there is a comparator that compares the values thus generated. Thus, the comparator in Mirov does not compare values that were *stored* in the read-only memory. Indeed, as Mirov relies on a data hash of the contents of the programmable memory, Mirov teaches away from the storage of a value for comparison; the value in the read-only memory cannot be altered when the contents of the programmable memory are changed.

Furthermore, Mirov, as can be seen from the passage above, relies on a comparison of a data hash (generated from the unsecured code in the programmable memory) with a verification hash (read from the programmable memory and generated based on the unsecured code in the programmable memory: see col. 4, lines 30-40, which describes that the digital signature is "encrypted from a secret key and the initial hash of the authorized programming micro-code"). Thus, the values compared by the comparator of Mirov are not *predetermined*; they are computed during initialization of the computer system.

Thus, the applicant submits that a *prima facie* case of obviousness has not been made out, because the cited prior art does not teach or suggest all of the elements of claim 1, nor of any of its dependent claims 2 through 7.

Similarly, the cited prior art does not teach or suggest all of the limitations of claim 18. The Examiner had drawn a similar conclusion with respect to the teachings of Mirov (Detailed Action, pages 9 and 10), although the Examiner had stated that "the signature [57] is interpreted to be independent from the contents of the FLASH memory because does not depend on the contents of the FLASH memory". That interpretation is incorrect in view of the description of Mirov as noted above, which states that the signature 57 is generated from a hash of the unsecured code in the PROM (col. 4, lines 35-40). Thus, for the same foregoing reasons, the applicant submits that no *prima facie* case of obviousness has been made out against claim 18, because the cited art does not teach and suggest all the elements of claim 18: there is no *predetermined* security value *stored* in read-only memory, as recited in claim 18. The applicant submits that the same reasoning applies to the program product claim 19.

The processor of independent claim 8 is recited therein to be configured to "execute boot program code... for comparing [a key value read from a security location in a flash memory] to a predetermined security value stored in the internal read-only memory". Thus, for the same reasons given above with respect to claim 1, the applicant submits that there is no *prima facie* case of obviousness made out, as the cited prior art does not teach or suggest all of the elements of claim 8, or its dependent claims 9 through 17: again, there is no comparison of any value to a *predetermined* security value *stored* in internal read-only memory, as recited in those claims, in the cited prior art.

Similarly, the cited prior art does not teach or suggest the elements of independent claim 20 for the same reasons: the cited prior art does not teach or suggest that any code may be executable on a processor to compare any value to a *predetermined* security value *stored* in the BootROM memory, as recited by claim 20.

There is no motivation to combine or modify Mirov with Cooper

Notwithstanding the foregoing, with respect to *all* pending claims the applicant respectfully traverses the Examiner's conclusion that a person having only ordinary skill in the art would have been motivated to "modify Mirov to include selectively polling a serial port based on a comparison of a key value if a flash ROM is corrupted as taught by Cooper" in order, as the Examiner stated, "to achieve the advantage of allowing a flash ROM to be updated to a known valid state even if the computer is unable to boot" (Detailed Action, page 3).

The Examiner has not identified anything in Mirov or Cooper that teaches or suggests that such a combination or modification of the cited prior art is desirable or achievable. Inasmuch as there is no teaching or suggestion in the Mirov or Cooper references themselves to so modify Mirov, the Examiner has apparently relied on the identification of an "advantage" to be realized as the motivation for modifying Mirov with Cooper. The applicant submits that this alleged motivation is improper for two reasons: first, the advantage identified is actually the advantage claimed by Cooper, and therefore a person skilled in the art seeking this advantage would have no motivation whatsoever to combine Mirov with Cooper, or modify Mirov with Cooper; secondly, to the extent that any advantage of the subject matter claimed in the currently presented claims of *this* application would have provided a motivating factor, the applicant submits that the

identification of this advantage is only possible through the impermissible application of hindsight.

The motivating factor identified in the Detailed Action is the achievement of:

> ... allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot. (Detailed Action, page 3)

However, Cooper itself states:

> In this manner, the flash ROM can be updated to a known valid state, even if the computer system is unable to boot up because of, among others, the corruption of the flash ROM. (col. 3, lines 23-26)

Thus, it appears that Cooper teaches the very "advantage" that is said in the Detailed Action to provide a motivation to modify Mirov with Cooper. In other words, there must not be any motivation *at all*, as Cooper apparently provides just what the person of ordinary skill in the art is said to have sought: "allowing a flash ROM to be updated to a known valid state even if the computer system is unable to boot." A person ordinarily skilled in the art, looking to provide a system that allows a flash ROM to be updated to a known valid state, would have no reason to modify Mirov with Cooper.

Therefore, on that basis, there is no motivation, teaching, suggestion, or any other inclination that has been identified that could lead to the modification of Mirov with Cooper. Thus, again, the applicant submits that there is no *prima facie* case of obviousness made out against the pending claims of this patent application.

Furthermore, the applicant respectfully submits that, to the extent that any advantage of the subject matter claimed in the currently presented claims of *this* application would have provided a motivating factor, the applicant submits that the identification of this advantage is only possible through the impermissible application of hindsight. In other words, *if* it could be argued that a modification of Mirov by Cooper would have been obvious in view of the recognized benefits of such a modification—which the applicant denies—it is submitted that the recognition of those advantages or benefits could only be accomplished by the application of knowledge gained from the present application. A skilled worker, looking forward from the appropriate date prior to the invention date of this application, would not have been motivated to make the stated modification in order to achieve the advantage of the claimed subject matter.

As no specific rejection based on motivation provided by an advantage of the present application has been made out in the Detailed Action, the applicant reserves the right to advance arguments and amendments, as necessary, to address such a rejection if one is made out.

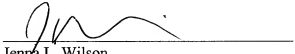
Moreover, there is no motivation to combine Mirov and Cooper to arrive at the claimed subject matter, as the prior art references are directed towards solving a different problem than what the present application teaches. The cited art is directed towards the problem of verifying or providing valid boot instructions; the subject matter of the currently pending claims is directed towards a security method that reduces the frequency of security breaches via an external port. The claims as amended reinforce this distinction by reciting two possible steps that are undertaken as a result of the comparison of the key and predetermined security values (i.e., to either poll the serial port for activity or jump to FLASH memory for execution of stored boot instructions).

The rejections of all pending claims were premised on the assumption that there was a motivation to modify Mirov with Cooper. Thus, for the foregoing reasons, the applicant respectfully submits that all claims, as amended, are non-obvious and patentable over Mirov in view of Cooper: not only do Mirov and Cooper fail to teach or suggest *all* of the elements of the pending claims, but there is no motivation to modify Mirov with Cooper.

No new subject matter has been added by this amendment. Favourable reconsideration and allowance of this application are respectfully requested.

Executed at Toronto, Ontario, Canada, on December 27, 2006.

RICHARD C. MADTER
RYAN J. HICKEY
CHRISTOPHER PATTENDEN



Jenna L. Wilson
Registration No. 54908
(416) 971-7202, Ext. 290
Customer Number: 38735

JLW:EDEV